

Potential System Vulnerabilities of a Network Enabled Force

Peter Houghton

Peter Houghton
Defence Science and Technology Laboratory (Dstl)
Dstl Malvern,
St Andrews Rd,
Malvern,
Worcestershire,
United Kingdom.
WR14 3PS

Telephone: +44 1684 77 1179
Fax: +44 1684 77 1437
E-mail: pdhoughton@dstl.gov.uk

© British Crown Copyright 2004 published with the permission of the Controller HMSO

This paper is the 11th in a set of 13 presented to the 9th ICCRTS by staff of the Defence Scientific and Technical Laboratory (Dstl) and QinetiQ plc, relating to 'command in the network enabled era'. The papers are based on research undertaken for the United Kingdom Ministry of Defence's 'Network Enabled Capability' programme and, unless otherwise stated, are covered in whole or in part by Crown Copyright.

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE SEP 2004		2. REPORT TYPE		3. DATES COVERED 00-00-2004 to 00-00-2004	
4. TITLE AND SUBTITLE Potential System Vulnerabilities of a Network Enabled Force			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defence Science and Technology Laboratory (Dstl),Dstl Malvern,St Andrews Road, Malvern,Worcestershire, United Kingdom, WR14 3PS, ,			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 49	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Potential Vulnerabilities of a Network Enabled Force

Peter Houghton

Defence Science and Technology Laboratory (Dstl)
Dstl Malvern,
St Andrews Rd,
Malvern,
Worcestershire,
United Kingdom.
WR14 3PS

© British Crown Copyright 2004 published with the permission of the Controller HMSO

This paper is the 11th in a set of 13 presented to the 9th ICCRTS by staff of the Defence Scientific and Technical Laboratory (Dstl) and QinetiQ plc, relating to 'command in the network enabled era', based on research undertaken for the United Kingdom Ministry of Defence's 'Network Enabled Capability' programme.

Abstract

The intent of the UK Network Enabled Capability (NEC) initiative is to gain military advantage through greater inter-working of organisations, people and equipment. It aims to achieve this by exploiting commercial sector information technology¹, and associated organisational concepts, and adapting them to the defence environment. However, the technology and associated concepts do not only confer benefits, they also bring with them penalties, risks and system vulnerabilities. Such penalties, risks and system vulnerabilities could potentially be very harmful, particularly if they occur at operationally critical times. It is thus imperative that the military and research communities remain vigilant, do not seek to emphasise only the positive and consider how such penalties and vulnerabilities might occur and how they might be mitigated.

This paper provides a brief review of some of the potential negative consequences of moving to a Network-Enabled future that have appeared in the open literature. As a consequence, this paper will not expose genuinely new or novel issues, particularly as the ground of vulnerabilities has previously been relatively well-trodden. However, it does attempt to aid those engaged in NCW endeavours in understanding the potential scale and extent of the problems they face, by bringing a number of the different sources and sets of issues together in a single place.

1 The Problem

NEC is a relatively new concept borne out of previous UK work, and that recently advanced by the US with the aligned concept of Network Centric Warfare. As with any new initiative, the focus of the work so far, has been the promotion of the new concept. When one is in this early phase of development, one tends not to explore too closely the potential negative consequences of embryonic concepts, as one is trying to advance new ideas and generate a degree of acceptance. However, as the net-centric concepts are now reaching a more established degree of acceptability, it is perhaps wise to start considering what some of their potential negative consequences might be.

We must also recognise that our opponents will not stand still. They will continue to exploit our weaknesses, and will be keen to locate them in any new concepts we develop and employ. They will specifically target these weaknesses and will intentionally avoid playing to our strengths. As quoted in a paper by Scherrer [1]:

"We must use all types, forms, and methods of force, and especially make more use of non-linear warfare and many types of information warfare methods which combine native and Western elements to use our strengths in order to attack the enemy's weaknesses, avoid being reactive, and strive for being active. In this way, it will be entirely possible for China to achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology."

General Wang Pufeng, Chinese Red Army

¹ Together with elements of bespoke government developed technology

1.1 *Our Response to the Problem*

Unless we deal with such negative consequences early, they are most likely to come back and impact on us more severely further downstream. We thus need to take the initiative and "grasp the nettle" with respect to these vulnerabilities. This requires us to:

- Develop an understanding of any potential weaknesses in our new approaches.
- Develop an understanding of how opposing forces might exploit such weaknesses.
- Develop an understanding of those weaknesses that may make us vulnerable to self-inflicted damage.
- Develop an understanding of how to reduce or eliminate our weaknesses or find ways to limit the ability of our opponents to exploit them.

First though, we have to accept that such weaknesses exist and second, we have to make a commitment to deal with them. This will require an investment of effort proportionate to the degree of risk that we perceive emanating from such vulnerabilities. There are a number of ways that a prioritisation of work on vulnerability might be made, one example being a risk assessment approach, such as that advocated by the US Army Research Labs [2].

1.2 *Sources of Criticism*

If we are to deal effectively with the vulnerabilities in NEC, it is necessary for us to take seriously any criticisms that are levelled at the concept.

"Network-centric warfare (NCW) increasingly is becoming a new orthodoxy - a set of beliefs that cannot be seriously challenged. Its disadvantages or critical vulnerabilities are not publicly discussed or are grudgingly admitted... The enemy rarely is mentioned, and he seems to be incapable of frustrating our plans and actions."

Dr. Milan Vego

As noted by Scherer, the vast majority of the criticisms seem to be related to four primary perspectives:

Historical - there are historical examples which demonstrate that hazards related to NCW do in practice generate undesirable outcomes. These historical contexts are arguably sufficiently similar with respect to "core" properties of net-enabled contexts that the lessons remain valid both today and in the future. For example, in Kosovo one could argue that the allies were in a state of near complete information superiority, yet this did not prevent them from being vulnerable to ingenious low-technology deception techniques conducted by Serbian armed forces.

National-strategic - Some of the NCW concepts appear to be at odds with requirements imposed by likely future strategic situations. For example, the emphasis on the support that NCW provides to sensor-to-shooter capabilities versus the need to engage more carefully and sensitively in peace-keeping and stabilisation operations.

Human-centric - there are many complex and detailed human factors issues that are easy to gloss over, but which could completely undermine the concepts if they are not attended to. Examples of some of these issues, that are referred to later in the paper, include the potential for loss of trust in information, loss of context and awareness of others' needs and reduction of social cohesion.

Science - (more specifically systems theories) - these theories suggest potential vulnerabilities, e.g. from the fields of complexity and chaos.

1.3 *Other Challenges*

Despite the value of the above categorisation from Scherrer, it is not complete. For example, NEC is challenged by issues emerging from at least two other prime perspectives. These are with respect to the technical challenges and those related to the philosophy of science being used.

Technical challenges surface from the inherent vulnerabilities in the technologies that are being used to construct the infrastructure supporting NEC. The second set of challenges emerges as a consequence of the particular philosophy of science being adhered to, in constructing the principles on which NEC is based. The technical challenges are not the focus of this particular paper, as these have been, and continue to be, researched in detail by specialist technical teams. However, the science challenges will be discussed later.

1.4 *Vulnerabilities, Susceptibility, Weaknesses and Risk*

It is all too easy to find oneself trapped in the midst of a pointless semantic argument regarding what a "vulnerability" is. Arguably, what is more important is to agree that there are a set of "things" that the defence community should collectively be worrying about. Whether you call these vulnerabilities, risks or design-constraints is less important than agreeing that they may cause us serious harm and that we urgently need to do something about them.

However, to pause briefly to consider what is intended by the concept of vulnerability: a dictionary definition is "*susceptibility to injury or attack*" or the "*state of being vulnerable*". To be vulnerable is to be "*capable of being wounded or hurt*" or "*susceptible to attack or physical or emotional injury*".

Vulnerability is thus a perceived weakness to injury, damage or attack. Injuries could of course be self-inflicted: e.g. one might argue that a vulnerability exists because we do not have a good Combat ID system, therefore we are vulnerable to blue-on-blue incidents. It is intended that all the concerns expressed in the paper relate to things of this nature: they point to potential weaknesses in our systems that either others can exploit or we may inadvertently trip-over ourselves.

One argument put forward is that it should be possible to separate risks (such as blue-on-blue) from vulnerabilities. However, vulnerabilities can also be considered as potential risks to an organisation, so the distinction can be difficult to make. As noted above, there

is an approach to vulnerability assessment [2] that uses a risk management approach based on the concept of susceptibility, although its focus is on equipment-type issues. In this approach, susceptibility is defined as a function of the potential damage caused by the vulnerability and the likelihood of whichever opponent we are facing being able to exploit that vulnerability.

Vulnerabilities may emerge from decisions and actions taken in many potential dimensions, for example, in respect of procedures, doctrine, equipment or indeed acquisition. For example, we may have a vulnerability in that we can be outpaced by forces who can rapidly assimilate and make use of the latest technology. The source of this vulnerability may be that we have acquisition systems that are too bureaucratic, slow, and cumbersome, which do not enable the holistic system innovation and evolution that we need to stay ahead.

Many of the various NEC/NCW critiques that this paper draws on can themselves be challenged from a number of perspectives. For example they may:

- Overstate, or take an extreme position, with respect to some of the NEC/NCW concepts in order to make their point.
- Paint a picture of future organisational situations that would arguably not exist in practice.
- Raise issues that are already in existence within military organisations and hence are not unique to network-centric organisational forms.
- Develop an argument based on incorrect expressions of fundamental principles and theories.

While many of these concerns are reasonable, the following observations are made:

- In order to think critically about something, it often requires extreme positions to be taken (or at least those which are out of the ordinary) to break out of cognitive traps².
- While logically it might appear nonsensical for certain organisational situations to exist, or conflicting states to exist simultaneously, one can still envisage specific circumstances where these might happen.
- While many of the vulnerabilities below could perhaps be applicable in a past or future without NEC, the move to a networked form may change the nature or severity of the concerns and thus they remain of interest³.
- There is less justification for the final challenge levelled at the critiques, that is, where they are based on an erroneous understanding of principles. However, as alluded to above, perhaps the most important value of all forms of critique, is that they trigger beneficial and important thought experiments. While the initial ideas supporting the critique may be in error, they may result in non-obvious lines of thinking, ones that

² See for example, *Serious Creativity*, DeBono, E., Harper Collins, 1992.

³ See table at Annex A, which attempts to define those vulnerabilities that are genuinely new concerns and those which may have already existed and NEC risks making worse.

perhaps provide additional insights and pointers to even more serious conceptual concerns.

In summary, one could apply an interpretation to the vulnerabilities listed below as pertaining to:

- Design constraints and choices: in that particular design decisions may be made which may make it more, or less likely that undesirable outcomes occur.
- System behaviours introduced by NEC that as yet are unknown.
- Risks that can perhaps be managed, for example by employing mitigation strategies.
- Weaknesses that can be exploited by our opponents.
- Weaknesses that are made worse, better, or changed in nature by a move to NEC⁴.

When examining each vulnerability in turn it is worth bearing in mind:

- Which particular model or variant of NEC it may apply to (accepting that we still have variety of possible models).
- Which particular point in the timeline of the evolution of NEC it is relevant to.

2 Analysis of Vulnerability Issues

The approach taken to the analysis of the potential vulnerability issues was as follows:

- A literature survey was conducted, which sought papers, books and reports that focussed either on a critique of NCW or discussed potential vulnerabilities. The vast majority of the relevant literature found relates to the US concept of Network Centric Warfare, not surprisingly as it came first, and because it has been much more widely publicised and discussed. While the two national concepts are different, the majority of the vulnerabilities discussed in the literature with respect to the US concept would appear to similarly apply to the UK NEC concept.
- A positive decision was made to try and locate a wide a range of issues, in order to provide breadth of coverage rather than, at this stage of analysis, providing significant depth. In any case, because of the relative immaturity of the concepts, it is likely that the depth of material simply does not exist in many areas.
- From each of the materials found, issues were extracted, collated and compared and brief discussion texts developed to summarise each separately identified issue.
- The issues were placed into a set of categories, which were developed by identifying similarities between the issues.

⁴ At Annex A is a table that suggests which of the weaknesses may already exist and which are potentially new as a result of NEC. Their likelihood is of course dependent on how NEC is eventually realised.

2.1 *Limitations of the Analysis*

First, it should be recognised that this analysis was bounded by the limited and finite time available. It should therefore be expected that many issues will be omitted, perhaps some of them significant. However, it is believed that the analysis does provide a reasonable coverage of the issues that are currently being openly discussed by both the operational and research communities.

Second, there is continued evolution of NEC and NCW, both in terms of their fundamental concepts and also in respect of how they are implemented. This analysis should thus be viewed as no more than a snapshot, at a particular point in time, of those issues that have been identified, and the expectation should be that new issues will emerge. Ideally, the topic of vulnerabilities requires long-term and continued effort, both to maintain awareness of the new issues as they arise and also to conduct work to lessen any potential impact.

2.2 *Classes of Vulnerability Issues*

As mentioned above, the vulnerabilities have been categorised to aid understanding. The following provides an outline of these categories, forming the structure of the following section that discusses each vulnerability issue in turn:

- Complex adaptive behaviour
- Technology imbalances
- Network reinforcing introversion
- Conflict between trend for platform sophistication and network resilience based on low value and ubiquity
- New information environment and pressures to respond
- Information processing
- Information operations including deception
- Effects on command and organisation
- Information risks

3 *Potential NEC Vulnerabilities*

3.1 *Introduction*

In an attempt to aid the reader who wishes to examine the referenced texts in more detail, references to supporting material have been added against each heading in turn. It will be noted that some headings have multiple entries, the reason being that the same issue was discussed in multiple sources. However, in the time available, it has not been possible to correlate all of the issues with the referred material, so unfortunately, some of the issues do not have a reference.

Finally, before stepping in to the detail of the issues, it is important to note that this analysis has not, in general, attempted to assess the merit or otherwise of the conceptual critiques⁵, for reasons explained in 1.4 above. The following therefore attempts to portray the issues as intended by the original authors. It is left as an exercise to readers, to apply their own judgement as to the value and correctness of each.

As noted above, while recognising that there are differences between UK NEC and US NCW, the similarities are such that the majority of the vulnerabilities apply equally to both concepts. As a consequence the terms NEC and NCW are used synonymously in the text below.

3.2 *Vulnerabilities arising from complex adaptive behaviour*

3.2.1 *Risks and Vulnerabilities of Complex Adaptive Behaviour* [1,6,8]

The potential benefits of complex adaptive systems are robustness, adaptability and flexibility over a wide range of situations. However, complexity science also suggests that changes in behaviour can be unpredictable and large in scale, and can result from relatively small changes in circumstances.

The vulnerability that this system property might expose for network centric forces is that they could be more sensitive than conventional forces to disruption. One could take two approaches to disrupt such systems. The first approach would be to deny inputs from the environment, which are necessary to allow the system to adapt. This denial will severely constrain the range of behaviours and options available to the organisation concerned. The second approach would be to deliberately insert inputs that are designed to drive an organisation into a chaotic state. For example, overloading sensor network grids, whilst simultaneously threatening use, or actual use of WMD and starting a cycle of frequent conventional or asymmetric attacks.

3.2.2 *Vulnerabilities arising from Self-Organisation and Synchronisation* [1]

There may be a fundamental conflict between self-organisation and synchronisation. Presently tactical forces are directed by operational-level command. If tactical level units are to take on more of the operational level responsibility and synchronise amongst themselves, then arguably they will need to conduct some of the activities previously carried out at the higher-level. However, it is unclear how tactical forces would be able to maintain an operational level perspective, so that they can formulate COA, consider enemy intentions, focus combat power and achieve the desired effects whilst remaining engaged in tactical combat. If one backs-off from the idea that tactical-level units can undertake all of these activities, it could be assumed that tactical units could potentially meet a smaller proportion of these requirements. This being the case, operational-level planners would have to take up the remainder of the burden, leading to the potential for serious divergence between them and the tactical units. In essence, operational level staff

⁵ Although some insightful observations from reviewers of early drafts of this paper have been included.

could be seeking to synchronise, in a deliberate planned manner, forces that are inherently un-synchronisable because of their self-organisation.

3.2.3 *Vulnerabilities of Network Effects* [1]

As a network grows, a point is likely to be reached where the addition of new users or new sources and data stores does not add value, but rather reduces it. For example, the network does not presently have unlimited capacity and therefore resource contention appears at some point. In addition, the volume of material and traffic on the information infrastructure makes it increasingly difficult to find the people and information that are relevant, as these are lost in the background noise. A phenomenon of network "clumping" also starts to emerge, where certain nodes start to accrete data, functions, traffic and value. If these valuable nodes are attacked, the network is found to be a lot less resilient than might be imagined. If the attacks are undertaken in an increasing and systematic fashion, backup services may also be overloaded, leading to complete infrastructure breakdown.

While we may be able to point to a single physical network, there is no one logical network, but instead a structure of human communities that is associated with the "clumping". As the resilience is dependent on the "clumping", one can infer that resilience is also dependent on the structure of the communities that form. As community structures unpredictably emerge, consequentially from the requirements of the operation and the individuals involved, it could be argued that the nature and degree of resilience of the infrastructure might itself be unpredictable.

3.3 *Vulnerabilities due to Technology Imbalances*

3.3.1 *Technology Differences Across the Coalition* [7,15]

NCW in its most extreme form is a path down which only the US can afford to go. Even close allies will be struggling to keep up and less affluent allies will be left straggling. The end result will be an even greater discrepancy between the abilities of coalition partners than exists today. If the US wishes to avoid coalition partners appearing only as non-credible, political symbols, then something will need to be done to ensure continued interoperability. This technology imbalance could also open up new vulnerabilities. For example, opponents could specifically target the fissures between coalition partners so as to deliberately create uncoordinated action, or heighten the perception of disharmony.

3.4 *Vulnerabilities due to the Network Reinforcing Introversion*

3.4.1 *Gaining Information Superiority may Disable Wider Communication* [7,10]

NCW may lead to an emphasis on greater internal networking relative to external networking. NCW seeks to gain information superiority, and thus one of the concepts is "locking out" your opponents from what is going on. However, in OOTW, the military need to be supporting others in the process of providing awareness and clarity about situations so as to provide a calming effect rather than a destabilising one.

The result of a strict adherence to internal networking may be to close down our own ability to communicate with opponents and allies. Such communication is vital, in order to start the process of conflict resolution. In addition, the actions taken against our opposition's information capability to gain information superiority may simply lead to an inflammation of an already difficult situation. In these situations one seeks non-lethal approaches, effects which are reversible, and keeping open channels of communication.

There is also the fact that, the more one disables an opposition's information infrastructure, the more difficult it becomes to determine their intentions and actions. In NCW, the rhetoric has highlighted the connection of sensors to shooters, rapid and decisive operations, shock and awe and closing down your opponents' ability to know what is going on. As a consequence, we may be generating concepts, doctrine and entrained responses in our military organisations that are the exact opposite of what is required for the majority of operations.

The potential for this vulnerability may only arise if we take too literally some of the rhetoric about information superiority. 'Locking out your opponents' ought to mean improved control over what does and does not get conveyed to other actors in the conflict space (including allies and neutrals). If one takes this particular stance, then having information superiority may actually mean having better control of the selective sharing of information.

Also, if we are really pursuing an effects-based approach, this should warn us to be extremely careful about how precisely we affect other actors information infrastructures, when the effects we may be seeking are to make their actions more predictable and determinable (e.g. from Signals Intelligence).

3.4.2 Self-Synchronisation Culture Could Damage Ability to Have Effective External Interaction

Self-synchronisation is an approach which, in general, is intended to provide increased agility and speed up the pace of the action. To achieve this, there is an emphasis on internal co-ordination as denoted by the term "self" i.e. it is the co-ordination of actions within our own organisation or with organisations with whom we are closely allied. Self-synchronisation works only because we have sufficient shared understanding of likely future actions by our colleagues. However, in the types of conflict that we are likely to find ourselves in the future, there will be a need for a more measured approach to decision making and action which needs to be inclusive of external, non-military stakeholders. Self-synchronisation in these circumstances could be wholly inappropriate. While one could argue that the simple solution is to only use self-synchronisation when it is appropriate, its implementation may lead to systems design, training and culture which is all orientated to internal working rather than inclusive external working with other agencies. The potential vulnerabilities that this might point to are being caught 'in the wrong mode' or in 'two minds' about which mode we are in. In other words, we may find our forces, in response to earlier and current operational needs, are engaged in tight self-synchronised activities when they also need to be engaging with external agents. One is then faced with a dilemma, in terms of which mode would be most effective (but not necessarily the safest) to operate in.

3.5 Conflict Between Trend for Platform Sophistication and Network Resilience that is Dependent on Low Value and Ubiquity

3.5.1 Sophisticated High Value Platforms as Nodes in Resilient Information Infrastructure [7,15]

NCW may be at odds with current trends in platform numbers and sophistication. Platform numbers, particularly in the air and maritime domains, have continued to decline along with increases in their technological sophistication. As a consequence, the value of each platform continues to increase and our need to protect them and keep them out of harm's way has also increased.

If we are to gain from the beneficial properties of a more pervasive and better interconnected network (in terms of reliability, resilience and effectiveness) we perhaps ought to be taking the opposite approach of procuring larger numbers of less sophisticated⁶ network nodes.

Many opponents are likely to be in an asymmetric position, having more platforms of lower value. They can thus use this numerical and value advantage to threaten our fewer more valuable platforms, potentially keeping them sidelined, or even worse, forced to retreat from the area of operations. If such platforms are also key nodes in our network infrastructure, we will have a simultaneous and serious loss of credibility and capability that will only encourage our opponents to continue the conflict.

3.6 Vulnerabilities Arising from the New Information Environment and Pressures to Respond

3.6.1 Increased Tempo Leading to Inappropriate Degree of Responsiveness [7,11]

One of the claimed advantages of moving to a network-centric organisation is that it will assist us in increasing our tempo so as to get inside opponents' decision making cycles. However, there is a danger that with the drive for increased tempo, combined with an increase in information collected, that we could end up reacting to events inappropriately. We could find ourselves in a position of responding to events so quickly that we are reacting to our own stimuli rather than responding to the actions of our opponents. Perhaps this relates to a type of failure in our perception of our opponents, one that leads to an erroneous attribution of intent, or potential, to them.

The network architecture has an advantage in the speed of processing and distribution of data. This advantage could either be used to inappropriately speed up reaction times, or it could be used to produce a more reasoned response⁷. The vulnerability or 'risk' is that we become seduced by the capability of the network to allow us to do things more quickly,

⁶ Or perhaps more correctly less-costly, as mass production of standardised components can allow the construction of quite sophisticated small to medium scale devices at low cost.

⁷ This problem has already been recognised by both the NEC community and the UK Joint Doctrine and Concepts Centre and is discussed in the UK High Level Operating Concept.

driven by concepts such as sensor-to-shooter and kill-chain, rather than taking a more considered and measured approach. We could thus end up "driving" situations in such a manner that we force our opponents into taking actions that are both undesirable and precipitative, and ones they would have avoided had we not so constrained them.

3.6.2 Increasing Information Load and Tempo Combined with Increased Lethality is a Dangerous Mix [6,7]

Technology is potentially increasing the complexity of the battlespace and making the task of command teams much more difficult. NCW will deliver a greater degree of information, not just in terms of amount, but also in terms of the "richness" of its content. It is likely to require a greater need for understanding of its meaning (for example, requiring greater knowledge of sensor capabilities). This need is amplified because the network has the capability to deliver much more information that arrives without its associated context.

At the same as the information load is increasing, the weapons systems at the commanders' disposal are also increasing in sophistication and are able to strike deeper, faster. Adding these two factors together, potentially drowns the commander with information and at the same time provides more opportunities for lethal action in shorter timeframes. With commanders increasingly under pressure to be seen to be taking action from the politicians and the media, this could lead to some dire consequences. One particular model of NCW, where there is a removal of procedures, and increased sharing of information combined with opportunistic use, could lead us to be particularly susceptible to this vulnerability.

3.6.3 Increasing Uncertainty and Reduced Time to Cope [11]

There are many changes occurring, which are increasing the uncertainty faced by Commanders⁸. First, commanders must now think, not just about own forces, but also what allies and other (perhaps non-defence) stakeholders might do in practice, as opposed to what was intended. Second, there are new weapons and systems, usually of greater sophistication than those they replace, entering service with own forces, allies and potential enemies, raising questions and doubts about how they will perform. New computers and sensors will increase many times the volume and types of information available to the commander, especially as digital devices become all-pervasive on the battlefield. The net effect of all these trends is a large increase in the uncertainty facing the commander. At the same time, the technology itself and the accompanying philosophies, doctrines and tactics may lead to increased tempo of operations. It could be argued that the military commander's need to balance his search for certainty, against the time available, is as old as the history of warfare. What is new is the large growth in uncertainty, coupled with the decrease in the time available to remove this uncertainty.

⁸ Note: this vulnerability has similarities with 3.6.2 above and 3.7.2, 3.95 below.

3.6.4 Dependence on Network, Tempo and Agility for Protection of Lighter Forces [5,15]

NCW has been offered as a route to coping with reduced defence budgets leading to lighter, more agile and less expensive forces. The claimed advantages of the use of the network such as better SA, pooling of dispersed resources through concepts such as network fires, greater agility and potential for increased tempo are crucial for this concept of lighter forces to retain any semblance of validity. However, precisely how the network does allow a smaller, lighter force to operate effectively and safely needs to be demonstrated. Specifically, if safety and effectiveness are dependent on operating at high-tempo, especially if driven by political pressure to be seen to be acting, this could lead to dangerous and precipitous action being taken. Conversely, having other agencies involved in the campaign, and especially in a multi-national context, the potential advantages of agility and tempo may not be attainable and our lighter forces could become extremely vulnerable.

3.7 Problems Arising from Information Processing

3.7.1 Common Operating Picture - impact on NEC benefits, its Subversion and Lack of Representation of Reality [6,10]

There is a particular train of thinking within NEC/NCW, which strongly relates the concept of providing better SA with the earlier concept of a Common Operating Picture (COP). While the COP concept is widely generally accepted, it is not without its critics, and previous studies have highlighted some of its potential undesirable effects. These effects could include information overload, and over-reliance on an erroneous abstract picture that is neither truly shared nor sufficiently representative of reality.

Having a picture which is perceived as "agreed" and "authorised"⁹ may also encourage control freaks, and turn the COP into a commander's "spin" on reality such that it becomes a "manipulated virtual reality". The focus should instead be on information "sufficiency" i.e. on what is needed by each function and level of command to get the job done, which includes determining the degree of necessary sharing and the degree of information consistency that is necessary for co-ordinated planning and action. Also required is a robust means of identifying inconsistencies between sets of shared information.

Simple-minded notions of what is meant by a COP could result in a force being "directed" by a need to create a single-pervasive view of reality that is both erroneous and slow to create. This potentially negates some of the potential advantages that NEC could provide such as agility and tempo, but also other benefits, such as more localised and tailored SA and the protection from deception obtained from a greater diversity of views of the battlespace.

⁹ A number of terms seem to be used synonymously to indicate that there is an authoritative view of reality that is being created, for example terms such as "recognised".

3.7.2 Information Management May Add to Uncertainties for Command [19]

The future information capabilities provided by NEC have the potential to "flood" consumers with information. The perceived answer to this problem is to simultaneously instigate information management. However, information management is itself not a panacea as information management processes and technologies may add further new uncertainties. For example, the commander may, as a result of information filtering instigated to provide a small body of relevant information, be presented with an overly "clean" picture of the situation. However, he may have little idea what information has gone into this picture, how reliable it is, what items of information have been combined with others, what kinds of mathematical processing of information may have been carried out, what information may have been discarded, and so on. The consequence of this is that we may have simply shifted the commanders' uncertainty from the operational situation to the information itself. We may find that he is less able to cope with this uncertainty than he was with the operational uncertainty.

It may thus be observed, that in the Information Age, the commander's ability exploit (rather than be dictated to, or misled by) his information resources will be a critical aspect of command. As noted above, the vulnerability implied here is that our commanders may not be good (or consistently good) at doing this.

3.7.3 Over-Reliance on Infrastructure and Lack of Ability to Exploit Reversionary Modes [6,8,9,19]

Conventional forces have used military concepts that cope with the difficulties created by poor connectivity: mission command¹⁰ being one of these. However, for a networked force, which relies upon connectivity for its "power", loss of connectivity could be nothing but disastrous. We are thus becoming increasingly reliant on the infrastructure, which becomes a primary centre of gravity for our opponents to exploit. Such weakness could become even more dangerous if "reversionary" modes (alternative ways of working) are not available. Such reversionary modes are not just technical in nature, they include the retention of skills that enable staff to operate without the technology. At some critical point, if the more manual modes of working are not continuously practised to aid retention, the consequent skill fade itself becomes a serious vulnerability.

3.7.4 Over-reliance on Remote ISTAR to Sustain Lighter Forces [9,10]

NCW has reinforced the move to lighter dispersed forces, with the argument being that we can make up for a loss in numbers and heavyweight forces and armour by being more agile and dispersed. One then uses the capabilities of the network to hook up to ISTAR and uses long-range targeting and strike capabilities to engage the heavier forces. Thus having lighter forces creates a strong reliance on these network capabilities, as one chooses not to engage lighter forces in short-range skirmishes, as they are too vulnerable.

¹⁰ Of course there are other reasons for employing mission command, such as generally being good leadership practice.

This approach makes us extremely vulnerable to deception, which has proven easy to conduct at low cost, as demonstrated in Kosovo operations¹¹. To add to the confusion generated by too heavy a reliance on ISTAR, military forces can be moved in small pieces, whilst at the same time refugee convoys are encouraged, and persuaded to use obvious military strategic routes increasing the concomitant risks of blue forces hitting civilians.

There are other disadvantages to remaining so far "out of contact" with the opposition. For example, the act of occupying ground causes your opponent to react, providing vital information regarding both his position and his intent. Remaining at a distance eliminates these opportunities to observe and learn.

3.8 *Information Operations Vulnerabilities Including Deception*

3.8.1 *Increased Susceptibility to Information Operations* [6,9,15,18]

Networked Forces could be particularly susceptible to Information Operations, which is an asymmetric approach that could be readily brought to bear by opponents with limited conventional military capability. Specific strategies can be employed, such as attacking our networks in a way that generates random failures in communications and information systems, with the intent to maximise the degree of uncertainty and confusion. Even a relatively simple approach, such as inserting random errors into information sources could have serious consequences. After a period of disruption, military staff would start to lose trust in the information systems and switch to much less effective (but perceptibly more reliable) information sources. These attacks may also generate increased use of insecure communications methods. Such methods can present a means of intelligence gathering to our opponents and simultaneously generate a degree of disorder in a networked force, which relies on cohesion and order to operate effectively. Capabilities that are heavily reliant on information could be severely disrupted if communication and information systems are disrupted; i.e. shared awareness, co-ordination, synchronisation and overall battlespace management could all be gravely affected.

3.8.2 *Increased Susceptibility from Use of Commercial Technologies* [3,9,19]

Military budgets are declining and the commercial sector drives the majority of technical advances. The result of this confluence is that the military finds it a necessity to adopt and adapt civil technologies to support the networked force. This creates a dependency both on the equipment and commercial service providers. The end result is that the military systems contain many of the same vulnerabilities as civil counterparts and hackers can readily transfer their skills to attacking similar military systems. The other danger is the low entry cost to sophisticated technology, which allows technically skilled organisations to develop, purchase and deploy precision weapons or inflict damage on information infrastructure e.g. low cost GPS jammers. One could legitimately argue that this is not a vulnerability that has arisen because of NEC, but rather existed some time beforehand. However, NCW and NEC are strongly based on the concept of exploiting

¹¹ As an example, towing 20-30 ft lengths of concertina wire can apparently deceive JSTARS.

some of the latest advances from the commercial sector. The point that is being made here is simply that any vulnerabilities which arise from commercial sector technology, applies particularly to the implementation of NCW and NEC.

3.8.3 *Sensor to Shooter Could Increase Susceptibility to Deception* [19]

To counter forces with advantages in technologies and firepower, alternative strategies are needed. These strategies allow one to avoid the firepower and prolong the conflict in an attempt to increase the cost to your opponent. A number of related approaches can be taken, firstly to disperse and conceal and secondly to deceive your opponent regarding your position, so as to expend their time, intelligence and ammunition on false targets. Both NCW and NEC are frequently linked strongly with concept of linking sensors to shooters. This potentially exacerbates the problems of countering these types of deception strategy, in that it may have a tendency to reduce the time and effort expended on distinguishing real from false targets and hence increasing vulnerability to deception. A potential weakness introduced by NEC/NCW is that the mechanisms for preserving sensor-to-shooter integrity are potentially bypassed, either by design misconceptions or by accident 'on the day'.

3.9 *Potential Effects on Command*

3.9.1 *NCW Could Make Command Failures More Pronounced* [11]

Using Pigeau and McCann's analysis of Command and Control (into the areas of Competency, Authority and Responsibility), it is possible to deduce potential impacts of NCW on Command [11]. For example, an increase in shared awareness of the battlespace and command intent has the potential to support commanders' personal authority. Conversely, where commanders exhibit questionable judgement this will be much more widely apparent and could help to undermine personal authority. In respect of intrinsic responsibility, an increase in shared awareness has the potential to be a strong motivating force to conduct effective action. However, awareness of some of the less optimistic assessments of potential outcomes could generate the opposite reaction. In the extreme, an awareness of particularly significant and serious events, if shared rapidly throughout a force, could induce an un-damped "shock" effect which temporarily disables the force while attention is being paid to the event, its potential consequences and divergent considerations about how to deal with them.

The above view of NEC/NCW is perhaps dependent on an overly optimistic view of our ability to share understanding of the operational and command situation. It could perhaps be equally argued that NEC/NCW might create informatic chaos, where no one really understands what is going on, and consequentially commanders' performance will be difficult to evaluate.

3.9.2 *Network Could Lead to Undesirable Shift in Balance Between Command and Control* [15,19,13]

A greater availability of information can lead to undesirable shifts in command authority. For example, providing information from sub-ordinate units can lead to over-control and micro-management. Conversely, providing a greater body of operational and strategic level information could lead to inappropriate pre-emptive action by subordinates. Determining what is appropriate and inappropriate will be difficult, as the very basis of self-synchronisation is to allow sub-ordinate units to make their own decisions in the context of the overall mission intent.

3.9.3 *Wider Information Availability leading to Inappropriate Decision Locations* [11,13]

By making information more accessible, there is an advantage that decisions can be made in locations that were previously impossible. However, there is a need to understand the balance between an ability to make a decision (now enabled by information) and the desirability of it being made in particular locations, by particular people. The vulnerability exposed here is that people who are neither skilled, authorised, trained nor sufficiently aware, may believe that they can take decisions because the network now provides some of the required information.

3.9.4 *Greater Diversity of Communication Paths Leading to Loss of Co-ordination* [13]

Potentially, the improved network interconnectivity provided by NEC/NCW will provide a means to route communications directly to key individuals and groups within the military enterprise. Organisationally, there is likely to be pressing need to use this technical capability. For example, if one is to increase both the "tempo of decision" and "tempo of action" then it will be necessary for information, requests and control to "skip" parts of the command organisation. This does not mean that "skipped" elements are not kept informed, but rather that it is ensured that they do not add unnecessary delays. However, there may remain a danger that such 'skipped echelons' are not 'kept in the loop' and as a consequence, co-ordination is lost along with a sense of being under-valued or under-utilised.

3.9.5 *Tempo and Decision Superiority Leading to High Workload and Fatigue* [11,13,15]

The need to attain information and decision superiority in combination with high-tempo, could lead to workload problems. If a continuous high-tempo cycle of sensemaking, assessment and decision making is required, there could be difficulties in containing workload within reasonable bounds, leading to command teams that become continuously fatigued. For many of the reasons explained elsewhere in this paper, NCW may add to workload and stress, due to increases in co-ordination, information load and uncertainty. When combined with many other factors operating in future conflict environments, this is likely to lead to much greater stress on commanders and command

teams. This stress could reach critical levels where command effectiveness drops off rapidly.

3.9.6 Dispersion and Technology Damaging Social Cohesion

NCW champions the concept of dispersed forces as a means to generate effects through approaches other than mass, to retain agility and to reduce vulnerability. However, such dispersion will inevitably challenge unit cohesion and bonding that has historically come from training and fighting together. This potentially impacts on some important necessities for command and co-ordinated group action such as leadership and trust. It could also negatively impact on agility, for example, how confident will military units be when they suddenly become critically dependent on people they have never worked with before? Future technologies may worsen this situation, for example video teleconferencing and robotics, if used inappropriately could increase the actual and perceived social separation of individuals, teams and organisations.

3.9.7 Agile Mission Grouping Damaging Social Cohesion

This is a slight variation on the vulnerability expressed in 3.9.6 above. If we have agility in mission group formation, with groups formed from the most suitable components available in the battlespace, different groups and personnel will be forced together. It will take time for these new groupings to achieve the social cohesion (and hence trust, shared awareness etc) before they are fully effective. This process will have to start again each time a new Agile Mission Group is formed. This could create weaknesses in our force as a result of a consequential slow-down in the pace of operations, a reduction of confidence in taking action and less effective co-ordination.

3.9.8 Information Availability Could Lead to Brittle Plans [13]

There is an assumption that simply providing more quality information will necessarily improve decision making. However, this assumption has probably not been tested comprehensively to attest to its validity. It might prove enlightening to conduct a series of experiments where the quantity of information provided to the commander (and/or the command team) is gradually increased, to see if this does indeed improve the outcome¹². It has previously been speculated that increasing information availability, might, at some threshold, lead to brittle and inflexible plans. The rationale for this is that when there is considerable uncertainty, commanders build in flexibility and contingencies. However, in an information rich environment, there may be a tendency to build much more rigid and more detailed plans based on an unhealthy belief in the certainty of the information provided. The mitigating factor may be that the sharing of plans through the network will hopefully lead to more robust solutions.

¹² Recent experimental work has clearly demonstrated that variations in the course of action chosen by military commanders may owe as much to internal moderators such as personality as to variations in the availability and quality of situation information.[22,23]

3.9.9 *Reliance on Information Superiority*

As a variation of 3.9.8 above, we are moving towards a situation where our entire concept of operations is based on the fact that the network will be able to gather (and distribute/ fuse/ deliver) the information we need. This will leave us very vulnerable when we come to fight a campaign where we are information poor. Examples might include fighting low level urban warfare in a country where we do not speak the language, do not understand the culture, and are distrusted by a significant proportion of the local populace.

3.10 *Potential Information Risks*

3.10.1 *Network Could Reduce Personal Sharing and Result in Loss of Required Context* [14]

The network allows much more sharing of data around the battlespace. Presently, data is frequently shared as a result of, or in combination with, person-to-person communication. This communication ensures that context is also shared and data is more likely to be correctly interpreted. However, in the networked environment, some of this contextual background may be lost and therefore there is a significantly increased risk of data being mis-interpreted. Meta-data has the potential to ameliorate this problem, but is likely to only treat the symptoms rather than be a lasting cure to the underlying problem.

3.10.2 *Network Could Reduce Awareness of Others and Lead to Loss of Co-ordination* [14]

Another advantage of personal communication is that it supports co-ordination i.e. the degree of awareness of what others are doing and why. Moving to a networked environment where a significant amount data is drawn from shared data stores, could paradoxically lead to a significant decrease in the awareness of own force intentions and actions. A deeper point about personal face-to-face communication is the development of empathy with one another, leading to more accurate assessment of what the other is really saying when you are apart. This might imply for example, a training regime rotating multi-national/force personnel to increase social contact.

3.10.3 *Network Could Increase Confusion in Coalition Environments*

Presently, information flows across allied boundaries in a restricted fashion, either through constrained gateways or through the manual efforts of liaison officers. While this creates bottlenecks, delays and loss of efficiency, it does tend to ensure that only interpretable information is exchanged and that misinterpretation of the meaning of data is reduced. If, in a networked force, there is a considerable improvement in connectivity and the volume of data exchanged between allies is vastly increased, this could simply lead to misinterpretation, greater confusion, even creating hostility between allies. It could also lead to yet further increases in the total volume of data through which people have to wade to find the material of relevance and value.

3.10.4 Network Could Reduce Necessary Diversity and Increase Susceptibility to Surprise and Deception [14]

The current breaks in our infrastructure reinforce a diversity of views and perceptions among components of our forces. Whilst this diversity could be seen as a drain on overall effectiveness, it is also a protection against deception and ensures that there is a greater degree of flexibility in our responses to unforeseen events. An increase in networking could also increase the degree of blinkered consensus and official groupthink within our forces and so dangerously reduce the degree of diversity. We may thus become much more vulnerable to deception and may not be able to respond so readily to the unexpected.

4 Scientific Challenges

4.1 Inductivism - a discredited approach

In a paper by Giffin[20], there is a discussion on the discredited scientific method called inductivism. Giffin controversially claims that many of the principles on which NEC and NCW are founded have emerged from this flawed philosophy. He explains that inductivism is based on three closely related tenets:

- The contention that the truth is manifest in nature - the truth is in the facts and that it will reveal itself to those who view the facts objectively.
- There is a logical process of probable inference - in that we can infer causes from effects, that is, we can induce more out of the facts than the mere facts.
- Characterisation of science as a quest for true and certain knowledge, with 'knowledge' defined as 'justified true belief'.

Viewed as a process, inductivism depicts science as a method with four key stages: objective observation, synthesis, justification and proof. By using the works of the two philosophers Hume and Popper, Giffin deconstructs each of the steps in turn and demonstrates that they do not have a sound basis. He concludes that they should therefore not be used as the basis for a scientific method.

As noted above, Giffin then argues that many of the principles that underpin, not just NEC and NCW, but the whole concept of the Revolution in Military Affairs (RMA) are based on this flawed method.

The critique of NCW is continued in a second paper by Giffin and Reid [21], which explains that their critical review on the NCW thesis has uncovered a range of problems that fall into two categories. The first category argues that the NCW thesis is based on an assembly of oversimplifications in a set of business analogies, a point which is also discussed by Kaufman[18]. The second category of problems is related to the discredited method explained above. However, in this later paper, the authors have moved beyond critique and have started the process of defining a new conceptual framework, one that they claim is based on sound scientific principles.

Regardless of arguments relating to inductivism, which many non-scientists may consider irrelevant, the military culture in which we operate appears to find the challenge of orthodoxy unacceptable. Over time the orthodoxy changes, but this is a slow and gradual process, during which time contrary views are suppressed. This same culture may ultimately also lead to the failure of NCW/NEC, as in order to implement it we need to challenge and overturn some well tried and embedded ways of doing business.

4.2 *Way forward*

There is not space in this paper to explain and discuss the entirety of the arguments put forward by Giffin, Reid and Kaufman. However, there are two key conclusions that are worth drawing out from examining their work.

First, that there is a school of thought emerging which challenges some of the fundamental principles of NEC and NCW. We should not seek to ignore or discredit such thinking, simply because it appears to undermine our current position. Rather we should seek to understand it in more detail to see if it has value and merit.

Second, and related to the first, is a scientific principle that tends to be eroded by inductive approaches, which is that of falsifiability and refutation. Simplifying greatly, this states that any theory of value should be potentially falsifiable i.e. there should be a means to be able to demonstrate that it does not hold. In fact, arguably, we should be applying as much effort in attempts to refute our theories and principles as we do to demonstrating them. Whether they withstand such tests is a secondary question, the first is that it is possible to devise such tests. Only by such a process will we gain any insight into whether they are robust or that they only hold under certain conditions. It is very important that we have this understanding, and that ideally we develop it in 'safe' experimental situations, rather than in the dangerous reality of operations.

5 Lessons Learned from Vietnam

Syvret[12] considered whether a digitized army of the kind now envisaged would have led the US to a different outcome in Vietnam. He examined the extent to which the advantages reportedly found for the digitized Task Force XXI in the Advanced Warfighting Experiment in 1997 would have been achievable in the Vietnam War.

It is worth pondering on the examples he provides of the more challenging aspects of this conflict:

- The heat, humidity, jungles and mountains of Vietnam in contrast to the dry plains of Texas and the implications for equipment reliability.
- The difficulty of detecting small groups of lightly equipped insurgents moving over thousands of trails under the cover of the jungle canopy in contrast to large numbers of highly visible armoured formations.
- The almost complete lack of high pay-off targets for high precision, high lethality (and high cost) weapons.

- The ability of the enemy to blend with the local civilian population (frequently there was no difference in Vietnam).
- The weight of IS equipment and its support requirements for soldiers deployed in a hostile environment.
- The tendency of senior commanders and politicians to use modern technology to adopt highly centralised decision-making.

This leaves us with many challenging questions, such as: What warnings does this provide us with, regarding the potential dangers and limitations of NCW approaches? How do we make sure that we do not have to learn similar lessons to Vietnam over again as a result of not thinking clearly enough about NCW vulnerabilities? How do we ensure that we deal with them effectively before we face them again in conflict?

6 Conclusions

It remains clear that Network-centric approaches have the potential to provide significant advantages for military capability.

However, in attaining these advantages there are some significant challenges to be overcome. These challenges may come from sources such as historical examples, national strategic demands, human factors limitations, and systems properties such as complexity and chaos. Previous vulnerabilities in equipment and systems, which have been of historic military concern will remain, and may if unchecked impact more severely in a networked environment.

There exists a body of sceptics, which is putting forward strong and convincing arguments that undermine some of the fundamental principles on which network-centric approaches are based. These arguments need to be considered carefully rather than dismissed or ignored because they are uncomfortable.

Even the sceptics accept that the emergence of information technologies has the potential to provide benefits. They also recognise that the NCW thesis has been of value in raising awareness of the potential benefits of information technologies, and in pointing out that there are useful insights that can be gained from examining business approaches. What they contend however, is that a more scientifically sound foundation is needed to guide the potentially large investments that will be made in the coming years.

This paper has highlighted some of the potential challenges and vulnerabilities and we ignore them at our peril. However, it is the product of a limited piece of research work, and represents only a snapshot of the situation at the current time. If we are to take the issues raised in this paper seriously a more concerted and enduring effort is required.

Finally, although not discussed in this paper, it is the author's view that work on vulnerabilities is presently very fragmented and that some benefit may thus accrue from creating a community of interest on the subject. The intent of forming this community would be to ascertain whether vulnerability issues can be addressed in a more holistic fashion than has hitherto been the case to date.

7 Recommendations

The analysis conducted in this paper should be conducted in a more comprehensive fashion and also be repeated on a regular basis to ensure that potential vulnerabilities are not missed. These may either be new vulnerabilities emerging or those that we have yet to identify.

There is a need for further analysis and experimentation to determine what the degree of risk is with respect to each of the potential vulnerabilities, to help focus our efforts on dealing with those that pose the greatest threat. This is not to say that all vulnerabilities are not important, it is just that some deserve more of our attention.

As NEC/NCW becomes normal business practice across our respective nations, there is a need to find a means for the practice of dealing with system vulnerabilities to also become accepted, and continually executed, standard practice.

We need to address the imbalance in our research, experimentation and exercises, such that they seek to expose and help to understand some of the mechanisms that could undermine NEC/NCW. Once this understanding is in place, we should seek to develop and test approaches to either eliminate such vulnerabilities, or more realistically, reduce their impact.

We should put forward plans for the conduct of experiments which attempt to refute some of the fundamental principles to demonstrate either their robustness or the limits of their application i.e. under what conditions do the principles hold.

It may be worth considering the development of the equivalent of a 'risk register' for such potential vulnerabilities, which includes the concept of a risk owner and details what our risk reduction strategies are. As with a risk register, risk owners should be regularly challenged to demonstrate that adequate steps continue to be made to address the concerns.

Consideration should be made to the creation of a 'community of interest' in NEC vulnerabilities, which attempts to develop a more holistic approach to dealing with the issues.

We should seek to understand the arguments put forward by some of the NEC/NCW sceptics, to determine for ourselves whether they are sound. This may require us to rethink some of our fundamental ideas behind NEC/NCW, but we should be always open to this. It may be that this will lead us to a different, but inherently more robust set of guidance for allied force transformation.

Annex A Table showing attribution of vulnerabilities

Each vulnerability is listed below with a view as to whether it existed in any significant form before NEC/NCW. In addition, the final two columns represent a very subjective impact analysis on each vulnerability. The intent of these two columns is not to state a definitive view backed up by evidence, but rather to suggest that a wider debate is needed on the vulnerabilities, their potential likelihood and impact.

Para	Vulnerability	Existing	New	Risk	Impact
3.2.1	Complex adaptive behaviour	X		M	H
3.2.2	Self organisation and synchronisation		X	L	M
3.2.3	Network effects			H	M
3.3.1	Technology differences across coalition	X		H	M
3.4.1	Gaining information superiority may disable wider communication	X		L	M
3.4.2	Self synchronisation culture could damage ability to have effective external interaction		X	L	M
3.5.1	Sophisticated high value platforms as nodes in resilient information infrastructure	X		H	H
3.6.1	Increased tempo leading to inappropriate degree of responsiveness	X		M	M
3.6.2	Increasing information load and tempo combined with increased lethality is a dangerous mix	X		M	H
3.6.3	Increasing uncertainty and reduced time to cope	X		M	M
3.6.4	Dependence on network, tempo and agility for protection of lighter forces	X		M	L
3.7.1	Common Operating Picture - impact on NEC benefits	X		H	M
3.7.2	Information management may lead to uncertainties for command	X		M	M
3.7.3	Over-reliance on infrastructure and lack of ability to exploit reversionary modes.	X		M	M
3.7.4	Over-reliance on remote ISTAR to sustain lighter forces	X		L	L
3.8.1	Increased susceptibility to information operations	X		M	H
3.8.2	Increased susceptibility from use of commercial technologies	X		M	M

3.8.3	Sensor to shooter could increase susceptibility to deception	X		M	H
3.9.1	NCW could make command failures more pronounced	X		L	M
3.9.2	Network could lead to undesirable shift in balance between command and control	X		M	M
3.9.4	Greater diversity of communication paths leads to loss of co-ordination		X	M	H
3.9.5	Tempo and decision superiority leading to high workload and fatigue	X		M	L
3.9.6	Dispersion and technology damaging social cohesion		X	M	M
3.9.7	Agile mission grouping damaging social cohesion		X	M	M
3.9.8	Information availability could lead to brittle plans	X		L	H
3.9.9	Reliance on information superiority	X		L	M
3.10.1	Network could reduce personal sharing and result in loss of required context		X	M	M
3.10.2	Network could reduce awareness of others and lead to loss of co-ordination		X	M	M
3.10.3	Network could increase confusion in coalition environments		X	M	M
3.10.4	Network could reduce diversity and increase susceptibility to surprise and deception		X	M	H

References

- 1 Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity, Scherrer, J.,H., Naval War College, February 2003.
- 2 Vulnerability Risk Assessment, Guzie, G.L., ARL-TR-1045, June 2000.
- 3 Induced Fragility in Information Age Warfare, Fowler, B.W., Peterson, D., R., ORMS Today, April 1997, Vol 24, No 2.
- 4 Where Did the Enemy Go?, Whither Warfare Symposium, Joint Doctrine and Concepts Centre, Shrivenham, April 2003.
- 5 Rapid Decisive Operations: The Emperor's New Clothes of Modern Warfare, Boling, J.,L., US Army War College.
- 6 The Coming Counterrevolution in Military Affairs, French, G., S., ICCRTS, 2003.
- 7 The Seven Deadly Sins of Network Centric Warfare, Barnett, P., M., US Naval Institute, (January issue pp. 36-39), 1999.
- 8 Network-Centric Warfare Requires a Closer Look, Blash, E., C., Lt Col., Signal, May 2003.
- 9 The Inherent Vulnerabilities of Technology: Insights from the National Training Center's Opposing Force, Rosenburger, J., D., Col, US Army.
- 10 War and Aftermath, Kagan, F., W., Policy Review, Jul-Aug 2003.
- 11 Command in a Network-Centric War, Forgues, P., Col., Canadian Military Journal, Summer 2001.
- 12 Would Information Age Forces have brought victory in Vietnam?: High Tech versus Low Tech on the 21st Century Battlefield, Syvret, M., Canadian Forces College, 1998.
- 13 21st Century Command, Comparison of Current Military Command Evolution and Potential Future Requirements, Houghton, P., Lomax, D. , unpublished DERA report, March 2001.
- 14 JOCS/JCSI Information Case Study Report, Houghton, P., Coles, D., unpublished DERA report, March 1998.
- 15 The Challenges and Limitations of "Network Centric Warfare" - The initial views of an NCW sceptic, Borgu. A., Network Centric Warfare: Improving ADF capabilities through Network Enabled Operations Conference, September 2003.
- 16 NCW Myths, http://www.dodccrp.org/NCW/ncw_myth.htm.
- 17 Networking in an uncertain world, Kaufman A., I., Journal of Battlefield Technology, Vol 5, No 3, November 2002.
- 18 Be careful what you wish for:The dangers of fighting with a network centric military, Kaufman A., I., Journal of Battlefield Technology, Vol 5, No 2, 2002.
- 19 Look Closely At Network-Centric Warfare, Col. Campen, A., D., USAF, Signal Magazine, January 2004.

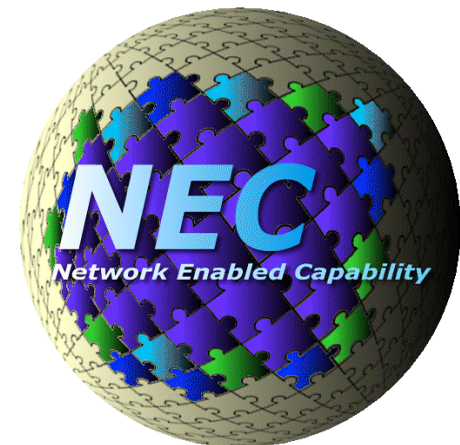
- 20 Superstitious Rituals: Naïve Inductivism in Command and Control Doctrine: Its Causes, Consequences and Cures, Giffin, R., E., 7th ICCRTS Symposium, Quebec, 2002.
- 21 A Woven Web of Guesses, Canto Three: Network Centric Warfare and the Virtuous Revolution, Reid, D., J., Giffin, R., E., 8th ICCRTS Symposium, Washington, 2003.
- 22 Malish, P., et al, Contribution of the Human Element to Command Effectiveness – The Impact of Information on Command Effectiveness, Defence Science and Technology Laboratory, Dstl/JA07514, June 2003 (awaiting publication).
- 23 Mathieson G. L., The impact of information on decision making, Defence Science and Technology Laboratory, DSTL/JA02207, presented at 18th International Symposium on Military Operational Research, August 2001.



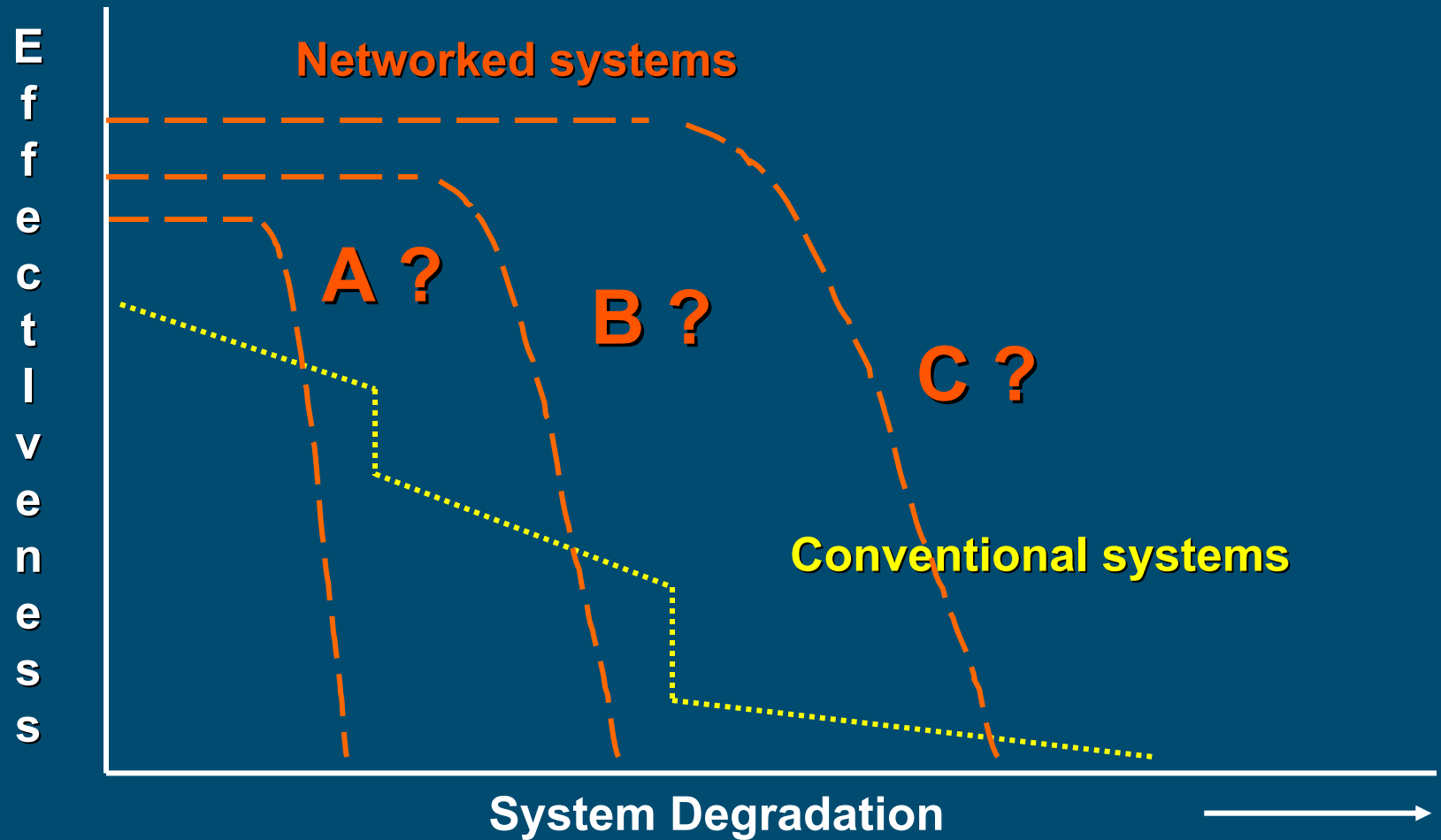
NEC Concepts - Risks and Vulnerabilities

Peter Houghton

9th ICCRTS, Copenhagen
14 September 2004



NEC - another proposition



NEC - Order of Magnitude changes?

- We tend to focus on the positive aspects of new initiatives
 - We forget that our opponents will continue to find ways to exploit weaknesses in any new approaches we develop (*they will specifically avoid playing to our strengths*)
- A warning from Scherrer¹:
 - ““We must use all types, forms, and methods of force, and especially make more use of non-linear warfare and many types of information warfare methods which combine native and Western elements to use our strengths in order to attack the enemy's weaknesses, avoid being reactive, and strive for being active. In this way, it will be entirely possible for China to **achieve comprehensive victory over the enemy even under the conditions of inferiority in information technology.**” - General Wang Pufeng, Chinese Red Army

Scherrer, J.H., Risks and Vulnerabilities of Network-Centric Forces: Insights from the Science of Complexity, Feb 2003.

3

Why consider NEC risks and vulnerabilities?

- Focus to date has been on promoting the concept, combined with advancing ideas and understanding
 - Arguably NEC concept is now sufficiently established
- Thus prudent to consider potential negative consequences of such an *approach*
- First we have to accept that such weaknesses exist and commit to dealing with them
 - Our opponents will not stand still - specifically they will avoid our strengths and target our weaknesses
 - Sceptics accept the potential benefits of IS technologies but contend that a more scientific foundation is needed for remainder
- Requires investment of a proportionate degree of effort

Scope

- Not technical vulnerabilities related to equipment
- Focuses on understanding the wider systems problems and concerns
 - Potential weaknesses in our approaches
 - How opposing forces might exploit such weaknesses
 - How those weaknesses may make us vulnerable to self-inflicted damage
 - Ways to reduce our weaknesses or to limit the ability of our opponents to exploit them
- Snapshot only

Other challenges

- Technical challenges
 - Inherent vulnerabilities in technologies
 - Inability of bureaucratic and slowly adapting defence organisations to acquire, assimilate, manage and use complex technology
- Challenges to maintain a 'scientific' approach to NEC development
 - Danger of focussing on evidence that supports our hypotheses of NEC benefits and discounting that which does not
 - Should be seeking with equal vigour and effort evidence that disproves our hypotheses
 - Otherwise we will not understand the limitations, risks and dangers in our proposed approaches

Understanding Weaknesses

- Requires us to take seriously criticisms levelled at NCW

"Network-centric warfare (NCW) increasingly is becoming a new orthodoxy - a set of beliefs that cannot be seriously challenged. Its disadvantages or critical vulnerabilities are not publicly discussed or are grudgingly admitted...The enemy rarely is mentioned, and he seems to be incapable of frustrating our plans and actions."

Dr. Milan Vego

- Time to:
 - Move away from beliefs or tenets to hypotheses that can be challenged
 - Publicly expose and discuss important vulnerabilities
 - Think more about how the enemy will exploit NEC/NCW weaknesses

Risk issues

- Risks and vulnerabilities arising from:
 1. Complex adaptive behaviour
 2. Technology imbalances
 3. Network reinforcing introversion
 4. Conflict between trend for platform sophistication and network resilience based on low value and ubiquity
 5. New information environment and pressures to respond
 6. Information processing
 7. Information operations including deception
 8. Effects on command
 9. Information risks

Note: Following slides are intentionally not a complete set due to need to keep within time bounds

3. Network Reinforces Introversion

- Information superiority may disable wider communication
 - NCW intent is to gain information superiority
 - Danger is greater focus on *internal* networking (“locking out” opponents - and potentially allies)
- Risks exposed - mainly in non-attritional conflict
 - Impair conflict resolution
 - Military need to be providing others with awareness and clarity of situations (calming rather than de-stabilising effect)
 - Attacks/degradation of opponents IS can both deny calming messages and inflame situations
 - Disabling an opponents information infrastructure can make it more difficult to discern opponents intent and actions

3. Network Reinforces Introversion

For example:

- Shock and Awe
 - Or ‘closing down your opponents ability to know what is happening’
 - May be generating entrained responses, doctrine that are the exact opposite of what is required
- Self Synchronisation
 - Largely, intended to exploit SA to better control tempo
 - Emphasis has to be on internal co-ordination (self!)
 - In future operations a measured approach is needed to decision making and action which include allies, and external non-military stakeholders
 - ‘Self’ synchronisation could be wholly inappropriate in these circumstances
 - Must be cognisant that we do not inadvertently develop a design, training and culture orientated to internal (only) working

10

4. Platform sophistication vs ubiquity

- NCW at odds with current trends in platform numbers and value
 - Platform numbers decline and 'value' increases
 - Opponents likely to be asymmetric with more platforms of lesser value
- Risks exposed
 - Need to protect platforms and possibly keep out of harm's way
- Exploitation approach
 - Opponents use numerical advantage to persuade high value platforms to retreat out of area
 - If high value platforms are also key infrastructure nodes - result is a simultaneous loss of capability and credibility

5. New Info env't & pressure to respond

- Increasing change in environment
 - Drive for increased tempo (to gain advantage)
 - Increasing amount of information collected (again to gain advantage)
- Risks exposed
 - Network architecture can provide advantage in speed and processing of data, hence:
 - could find ourselves responding to events so quickly - responding essentially to our *own stimuli*
 - may inadvertently take precipitative action and drive operation into more dangerous and precarious states

6. Information Processing

- Over-reliance on COP - an erroneous abstract picture that is neither truly shared or sufficiently representative?
 - Temptation for Command teams to be presented with “clean”, processed and filtered data
- Information management and processing could add new uncertainties
 - Little knowledge of the data sources and subsequent processing
- Risks exposed
 - Consumers have little idea what data has gone into ‘picture’, how reliable it is, what has been fused, what types of math’ processing conducted, what data may have been discarded
 - Uncertainty is shifted from operational situation to the data itself

7. Information Operations

- To counter capable forces with technology and firepower advantages opponents increasingly employ asymmetric approaches
 - (To avoid firepower) including targetting of our infrastructure
- Risks exposed by opponents' asymmetric approaches
 - NEC concepts rely on connectivity - over-reliance on infrastructure, lack of 'reversionary' modes
 - Opponents introduce random failures e.g. via hacking
- Exploitation approach
 - Aim of opponents is to prolong conflict and increase cost e.g. expend blue force time, intelligence and weapons on false targets

9. General Information Risks

- Network could reduce personal sharing and loss of required *context*
 - Network allows much greater sharing of information
 - Presently data is frequently shared during interpersonal communication
 - This ensures context is shared and gradually built up and data is more likely to be correctly interpreted and errors quickly detected
- Risks exposed
 - In networked environment - impersonal sharing may lead to loss of important context
 - Significant increased risk of data misinterpretation - especially in coalitions
 - Error detection processes reduced

Conclusions

- Network-centric approaches have the potential to provide significant advantages
- However, there are also serious potential 'downsides'
 - Challenges from systems, technical and science perspectives
- We ignore these risks, challenges and vulnerabilities at our peril
 - We need to understand the nature and severity of these risks and the conditions under which they become activated
 - Their likelihood, impact and importance has yet to be substantially investigated
 - We need to accept that such vulnerabilities exist, develop and test approaches to eliminate them or at least reduce their impact

Future Research

- There is a need to:
 - Identify more comprehensively system-level risks and vulnerabilities
 - Understand relationship to NEC implementation decisions and feed the warnings into the appropriate decision making processes - including links with experimentation
 - Understand what preventative or mitigating measures are necessary and ensure that appropriate advice is provided to the NEC delivery process
- Previous focus on system-level
 - Need to consider more technical, component level issues
 - Determine whether these have localised or system-wide effects e.g. compromise of communications affecting trust in info source

Important Issues

- To resolve vulnerabilities and risks will require co-ordinated effort across all Lines of Development
 - e.g. password - technical solution to social engineering
- Will require a continuous “learning from experience” process
 - Understand from practice as well as analysis which are the important ones to focus on
 - Understand whether mitigating measures work effectively
 - Look out for indicators of previously unrecognised vulnerabilities
- What are the different types of asymmetry that might be employed against us?
 - Does this generate new vulnerabilities or change our view on current ones?

Questions?

Candidate Research Questions (1)

- 1. Does complexity science provide us with insights into potential vulnerabilities?
- 2. Is it possible to develop an 'integrated' force where components have different degrees of net-centricity?
- 3. Is it possible to exploit information superiority without reducing the effectiveness of our external communication?
- 4. How do we deal with the trend towards reduced platform numbers and the networked ideal of greater numbers?
- 5. How do we ensure that networked forces select appropriate tempo, do not get driven by own stimulus, and spend sufficient time making sense of greater input volume?
- 6. How do we ensure that our 'information improvements' do not simply increase stress, workload and uncertainty for command?

Candidate Research Questions (2)

- 7. What are the best approaches for protection against IO - not just against technology attacks?
- 8. How do we ensure that the network does not amplify damaging effects of poor command?
- 9. How do we ensure that greater use of automation for information sharing does not lead to damaging loss of necessary context?
- 10. What training do we provide operational and support staffs to avoid the NCW hazards?